IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	**Crim. No. 1:12-CR-267**
	:	
	:	
v.	:	
	:	
DARIUSZ PRUGAR	:	
	:	**Judge Sylvia H. Rambo**

M E M O R A N D U M

Presently before the court is Defendant Dariusz Prugar's ("Defendant") motion to vacate, set aside, or correct sentence pursuant to 28 U.S.C. § 2255. (Docs. 138-39.) Defendant argues that he presented his counsel at trial with exculpatory evidence and that counsel unreasonably refused or failed to offer such evidence to the jury or otherwise failed to properly investigate such evidence. For the reasons that follow, Defendant's motion will be denied.

I. Background

On March 11, 2016, Defendant was convicted on one count of Intentional Damage to a Protected Computer in violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(5)(A) and one count of Wire Fraud in violation of 18 U.S.C. § 1343. (Doc. 95.) That same day, Defendant was found not guilty of Interference with Commerce by Threat of Violence in violation of 18 U.S.C. § 1951. (*Id.*) On November 29, 2016, Defendant was sentenced to serve a total of 24 months' imprisonment and three years of supervised release and

directed to pay restitution in the amount of $26,942.86 in addition to $200 in special assessments. (Doc. 122.) Defendant does not dispute that he committed the acts giving rise to the crimes with which he was charged. Defendant instead raises a factual dispute regarding the harm resulting from his actions. Specifically, Defendant admits that he accessed his former employer's computer network without authorization. Defendant, however, posits that his actions could not have caused the resulting damage to the victim's computer network, and it amounts to no more than poor fortune that the victim's financial loss occurred a short time after Defendant's intrusion into the network. The facts underlying his conviction are as follows.

From 2008 to 2010, Defendant was employed by Netrepid, a computer and internet service provider, as the engineer acting as custodian of Netrepid's network infrastructure. As the custodian and architect of the system, Defendant "was the only one that knew how the network worked." (Trial Transcript ("TR.") at 131.) In early 2010, Netrepid instructed Defendant to begin to train two newly hired employees on how to maintain the network and share the necessary passwords with those employees. Defendant, however, refused to grant or limited access to the network, leaving the new hires "effectively blind" without him. (*Id.* at 87.) On June 25, 2010, Netrepid terminated Defendant's employment. That same day, Netrepid hired an independent contractor to change the network passwords in an

effort to prevent Defendant from accessing the network after the date of his termination. Netrepid's efforts apparently failed in this regard. On the night of Friday, June 25, 2010, Defendant gained access to the Netrepid network from a remote location, using his knowledge of the network's security operations.[1] Defendant testified that his unauthorized entry was in an effort to obtain data or files that he considered his own intellectual property, which he believed Netrepid would refuse to hand over. After retrieving the desired files, Defendant deleted "log" files, which are essentially records of which users logged into the system and the actions those users carried out while logged on. Defendant purportedly deleted the log files in an effort to conceal the fact that he had gained unauthorized access to the network. After deleting the files, Defendant logged off the system. At this point, the facts presented to the jury and the facts averred by Defendant in his Section 2255 motion begin to differ.

[1] Defendant takes issue with the colloquialism "back door" used to describe his method of entry into Netrepid's network. Generally, this term is used to describe a hidden access point to a network that was created for the specific purpose of accessing a system covertly. In his post-hearing brief, Defendant avers that the entry he used was "visible to everyone who had access to the system" and that "his Netrepid credentials [] had not been disabled after he was fired." (Doc. 173, p. 18 (citing Doc. 173-1, p. 125).) Defendant appears to contradict his own testimony by stating that he created a separate and anonymous user name, "system," which was known only to him. (*Id.* at pp. 18-19 (citing Doc. 173-1, p. 125).) Although Defendant notes that the user name "system" was visible on the list of all authorized user names, the innocuous title and the fact that Netrepid was not made aware that Defendant created the user name for his own use appears designed to obscure the fact that it was effectively a secondary account used only by Defendant. Regardless of the terminology used to describe it, Defendant unequivocally accessed Netrepid's system with the full knowledge that he was no longer authorized to do so. Moreover, the fact that the point of entry was "visible to everyone" is irrelevant, especially considering the consistent testimony that Defendant was the only individual with a complete understanding of how the network functioned.

At trial, the Government presented witnesses who were experts in the fields of computer science and programming. These witnesses testified that the deletion of the log files created a "domino effect," whereby the entire internet network operated by Netrepid crashed, *i.e.* ceased to provide internet service to Netrepid's customers. In sum, the "domino effect" described by the Government's experts occurred when certain programs essential to the network's operation sought the log files deleted by Defendant. Because these essential programs could not locate the deleted files, those programs crashed. The crash of those programs, in turn, caused other programs to crash, until the entire network was rendered inoperable. While investigating the cause of the crash and attempting to correct the problem, Netrepid discovered the unauthorized access and referred the matter to local police who then referred it to the Federal Bureau of Investigations ("FBI"). The FBI began its investigation by interviewing Defendant and other former and current employees. In the course of their interview, Defendant admitted to accessing the network without authorization.

Defendant was charged by indictment on October 17, 2012, (Doc. 1,) and initially entered a plea of not guilty, (Doc. 11). On February 19, 2013, Defendant changed his plea of not guilty to guilty. (Docs. 29, 30.) After retaining trial counsel, Defendant filed a motion to withdraw his guilty plea on June 6, 2014. (Doc. 38.) After briefing and a hearing, Defendant's motion to withdraw his guilty

plea was initially denied by order dated September 22, 2014. (Doc. 52.) The court, however, granted reconsideration *sua sponte* of Defendant's motion to withdraw his guilty plea, finding that there was sufficient evidence to support Defendant's claimed defense to justify Defendant's request. (Docs. 76, 77.) The matter then proceeded to trial which was held between March 7 and March 11, 2016. As noted above, the jury returned a verdict of guilty on counts one and two of the indictment, and a verdict of not guilty on count three. (Doc. 95.) Defendant subsequently filed a motion for acquittal or a new trial on March 25, 2016, (Doc. 106,) which was denied by order dated May 15, 2016, (Doc. 110). Defendant was sentenced on November 30, 2016. (Doc. 122.) Defendant subsequently appealed from the judgment of sentence on December 9, 2016, (Doc. 126,) and said appeal was dismissed on February 17, 2017, (Doc. 135). On November 28, 2017, Defendant filed the instant motion to vacate, set aside, or correct sentence. (Doc. 138.)

In his motion, Defendant argues that trial counsel was ineffective for failing to present evidence demonstrating that the crash experienced by Netrepid could not have been caused by the deletion of the log files. In support of this theory, Defendant planned to (1) testify to that effect; (2) present a diagram of the network configuration to the jury; (3) present a page from the system's operating manual that allegedly would demonstrate that the harm could not result from the deletion

of log files; and (4) present phone records indicating that the network crash occurred several days after his intrusion. Defendant alleges that he informed his trial counsel, Royce Morris, Esquire,[2] of this exonerating evidence, yet trial counsel strongly discouraged him from testifying, did not present the diagram, phone records, or manual as evidence, and failed to adequately investigate Defendant's proposed theory. An evidentiary hearing on Defendant's motion was held on June 13, 2018. Accordingly, the matter is now fully briefed and is ripe for disposition.

II. Legal Standard

Under Section 2255, a federal prisoner may move the sentencing court to vacate, set aside, or correct the prisoner's sentence. 28 U.S.C. § 2255. Courts may afford relief under Section 2255 on a number of grounds including, *inter alia,* "that the sentence was imposed in violation of the Constitution or the laws of the United States." *Id.* at § 2255(a). The statute provides that, as a remedy for an unlawfully imposed sentence, "the court shall vacate and set the judgment aside and shall discharge the prisoner or resentence him or grant a new trial or correct the sentence as may appear appropriate." 28 U.S.C. § 2255(b). The court accepts the truth of the defendant's allegations when reviewing a Section 2255 motion unless those

[2] In the time between Defendant's conviction and the filing of Defendant's motion, trial counsel was elected as a judge of the Court of Common Pleas of Dauphin County. Herein, the court will refer to Judge Morris in his capacity as "trial counsel" during the relevant proceedings.

allegations are "clearly frivolous based on the existing record." *United States v. Booth*, 432 F.3d 542, 545 (3d Cir. 2005). A court is required to hold an evidentiary hearing when the motion "allege[s] any facts warranting § 2255 relief that are not clearly resolved by the record." *United States v. Tolliver*, 800 F.3d 138, 141 (3d Cir. 2015) (quoting *Booth*, 432 F.3d at 546).

III. Discussion

A. Damage versus Financial Loss

Preliminarily, the court will dispose of the Government's argument that the court need not determine whether Defendant's intrusion into the network caused the overall system crash and service outage because the deletion of data files alone qualifies as "damage" under the CFAA. The court rejects this argument. Under Section 5(A) of the CFAA, a defendant must be found to have "knowingly cause[d] the transmission of a program, information, code, or command, [that] intentionally cause[d] damage without authorization, to a protected computer." 18 U.S.C. § 1030 (5)(A). Although the government is correct that the legal definition of "damage" under the CFAA includes the deletion of files,[3] and Defendant unequivocally states that he did so, the statute does not contemplate a felony

[3] Under the CFAA, the "term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information;" and "the term 'loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(8), (11).

conviction for *de minimis* damages. For sentences of one year or more, the statute imposes a floor of $5,000 in damage: "The punishment for an offense under [S]ection [5(A)] is . . . a fine under this title, imprisonment for not more than 10 years, or both, in the case of:"

> (i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)--
>
> (I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
>
> (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
>
> (III) physical injury to any person;
>
> (IV) a threat to public health or safety;
>
> (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or
>
> (VI) damage affecting 10 or more protected computers during any 1-year period; or
>
> (ii) an attempt to commit an offense punishable under this subparagraph;

18 U.S.C. § 1030(c)(4)(A).[4] If none of those enumerated harms are present, Section 1030(c)(4)(G) provides that the appropriate sentence shall be "a fine under

[4] Section 1030(c)(4)(B) relates to the sentence imposed for an offense under Section (a)(5)(A) of the CFAA; however, Section (c)(4)(B) refers to the "harm provided in subclauses (I) through (VI) of subparagraph [(c)(4)](A)(i)." Thus, the requirements for a felony offense under Section

this title, imprisonment for not more than 1 year, or both, for (i) any other offense under subsection (a)(5)." Without accounting for the costs to rebuild the Netrepid network, the Government presented no evidence of the financial loss attributable to the deletion of log files alone. In all likelihood, if Defendant is correct that the deletion of the log files did not cause the system crash, there would be no appreciable financial loss to Netrepid.

The Government is correct to the extent that it argues that Defendant would likely have been found guilty of a felony offense under a separate subsection of the CFAA, regardless of the arguments raised in his Section 2255 motion. The court, however, must still analyze Defendant's arguments to determine if a resentencing or amended sentence is required. Defendant was also found to have caused "damage affecting 10 or more protected computers" in violation of 18 U.S.C. § 1030(c)(4)(A)(i)(VI), which would also qualify as a felony offense. As discussed, *infra*, the court does not find that counsel was ineffective, and, even if the court did so find, Defendant raises no arguments contradicting his conviction under 18 U.S.C. § 1030(c)(4)(A)(i)(VI). Thus, a resentencing would be appropriate predominantly to reconsider the amount of restitution owed by Defendant. Because Defendant's sentence is predicated on the damage and financial loss attributable to his actions, *i.e.*, the entry into the network and the deletion of log

(a)(5)(A) and (a)(5)(B) are the same insofar as both require one of the enumerated harms under Section (c)(4)(A)(i).

files, the court must address whether Defendant's trial counsel was ineffective for failing to present evidence which may have shown that Defendant's actions could not have caused the total financial loss suffered by Netrepid.

B. Ineffective Assistance of Counsel

A collateral attack based on ineffective assistance of counsel is governed by the two-pronged test established in *Strickland v. Washington*, 466 U.S. 668 (1984). Under the *Strickland* test, a defendant must demonstrate that (1) counsel's representation fell below an objective level of reasonableness based on prevailing professional norms, and (2) the deficient representation was prejudicial. *See id.* at 687-88. The defendant bears the burden of proving both prongs. *See id.* at 687. Conclusory allegations are insufficient to entitle a defendant to relief under Section 2255. *See United States v. Thomas*, 221 F.3d 430, 437 (3d Cir. 2000).

In determining whether counsel has satisfied the objective standard of reasonableness under the first prong, courts must be highly deferential toward counsel's conduct. *Strickland*, 466 U.S. at 689. There is a strong presumption that counsel's performance falls within the wide range of reasonable professional assistance. *See United States v. Gray*, 878 F.2d 702, 710 (3d Cir. 1989). Only a "rare claim" of ineffectiveness of counsel should succeed "under the properly deferential standard to be applied in scrutinizing counsel's performance." *Id.* at 711 (citing *Strickland*, 466 U.S. at 689-90).

To satisfy the prejudice prong, the defendant must establish a reasonable probability that, but for counsel's errors, the outcome of the proceeding would have been different. *See Strickland*, 466 U.S. at 694. "A reasonable probability is a probability sufficient to undermine the confidence in the outcome." *Id.* at 694. "The likelihood of a different result must be substantial, not just conceivable." *Harrington v. Richter*, 562 U.S. 86, 112 (2011). The district court need not conduct its analysis of the two prongs in a particular order or even address both prongs of the inquiry if the defendant makes an insufficient showing in one. *United States v. Lilly*, 536 F.3d 190, 196 (3d Cir. 2008).

Defendant advances two theories in support of his request for Section 2255 relief: (1) trial counsel made a prejudicial error by strongly urging Defendant not to testify on his own behalf; and (2) trial counsel failed to satisfy his duty to investigate or present potentially exculpatory evidence.

I. Trial counsel's advice not to testify

Bound up in Defendant's argument that trial counsel erred in advising him not to testify on his own behalf is the argument that trial counsel so strongly urged Defendant not to testify that trial counsel's advice amounted to coercion and a deprivation of Defendant's constitutional rights. The Supreme Court has held that the right to testify on one's own behalf is rooted in three separate provisions of the Constitution. *Rock v. Arkansas*, 483 U.S. 44, 51, (1987) (holding that the

"Fourteenth Amendment's guarantee that no one shall be deprived of liberty without due process of law include[s] a right to be heard and to offer testimony."); *Washington v. Texas*, 388 U.S. 14, 17–19 (1967) (holding that the right to testify on one's own behalf is included in a defendant's "right to call 'witnesses in his favor'" created by the Sixth Amendment's Compulsory Process Clause); *Harris v. New York*, 401 U.S. 222, 225 (1971) (holding that the Fifth Amendment provides that "[e]very criminal defendant is privileged to testify in his own defense, or to refuse to do so."). A defendant's right to testify on his own behalf is not a mandate, however, and there are myriad reasons why a defendant may choose, and counsel may advise, to invoke the Fifth Amendment right not to testify. The court's investigation on this issue is twofold. First, did Defendant present evidence that would demonstrate that his trial counsel coerced him into giving up against his will his constitutional right to testify on his own behalf. Second, if counsel's advice not to testify did not amount to coercion, was it unreasonable in light of the potential testimony offered by Defendant.

In determining whether defense counsel unduly coerced a defendant into waiving his right to trial, courts have distinguished between situations where a defendant expressed initial hesitation in waiving the right to testify in his defense, yet ultimately acquiesced to his counsel's advice and those cases where counsel flatly refused to allow the defendant to testify or erroneously informed the

defendant that he had no such right. *United States v. Mullins*, 315 F.3d 449, 455 (5th Cir. 2002) (concluding that trial counsel was ineffective where "[t]he district court found that both [defendant] and his trial counsel 'testified credibly at the evidentiary hearing that [defendant] expressed a desire to testify [to his counsel] numerous times during trial and that counsel alone chose to prevent his testimony."). The evidence before this court is quite different from the evidence in *Mullins*. Not only did trial counsel fail to corroborate Defendant's assertion that he was coerced into not testifying, Defendant appears to admit that he knowingly acquiesced to trial counsel's advice.

Defendant testified that trial counsel advised him that: "You know, the worst thing a trial attorney can have is for his client to take the stand and for the case to fall apart, and it doesn't seem like you have the ability to take the stand." (Doc. 173-1, p. 195.) Upon further questioning, Defendant explained his understanding of trial counsel's comment:

> Q. And what was your understanding of that comment?
>
> A. The way it came across was a vote of no confidence, like I would do more harm than help.
>
> Q. Did your decision not to testify, was it based on the advice of [trial counsel]?
>
> A. Yes.
>
> . . . .
>
> Q. And again what was your view of [trial counsel]'s opinion regarding you testifying?
>
> A. It appeared to be a decision telling he wasn't going to let me testify.

> ….
>
> Thank you, Your Honor. Just with that last answer [Defendant], you just said that [trial counsel] was not going to let you testify. Is that an accurate statement of what happened?
>
> A. His language came across as if you wanna go for it, but I wouldn't do it, that kind of thing. So the language may not have been you're not going to do it, but the message certainly was.
>
> Q. The message wasn't though he's not going to let you testify. The message was it's his recommendation that you do not testify, but that it's your choice?
>
> A. Exceedingly strong recommendation to not take the stand.
>
> Q. But it was your choice?
>
> A. Upon his recommendation.

(*Id.* at 195-97.) Although Defendant now views trial counsel's recommendation as "exceedingly strong," he admits that he chose not to testify upon such recommendation. Moreover, Defendant's fiancé, who attended most, if not all, of the defense preparation meetings between Defendant and trial counsel, testified similarly:

> Q. And you testified on cross examination a moment ago that the decision to testify was ultimately [Defendant]'s, isn't that right?
>
> A. Yes.
>
> Q. And was it your understanding from that Wednesday evening meeting that [Defendant] understood the decision of whether to testify or not was his?
>
> A. Yes.
>
> Q. Did [trial counsel] provide that legal advice to [Defendant] that the decision to testify was ultimately his, being [Defendant]'s?
>
> A. Yes.

(*Id.* at 29-30.)

> Q. Based on your interactions with [Defendant], what was your understanding of whether or not his counsel wanted him to testify?
>
> A. It was my understanding that—I don't know if I got the question, but it was my understanding that [trial counsel] strongly advised [Defendant] against testifying.

(*Id.* at 51.) Accordingly, Defendant has presented no evidence that he was, either objectively or subjectively, coerced into giving up his constitutional right to testify on his own behalf. The testimony is clear that Defendant initially desired to testify, listened to trial counsel's advice to the contrary, and knowingly acquiesced to counsel's advice. "Trial counsel's performance is not constitutionally deficient where counsel advises the defendant of his right to testify, but also advises defendant that he should not exercise that right because it would be unwise." *Greer v. Harlow*, No. 12-cv-1263, 2015 WL 5730787, *15 (W.D. Pa. Sept. 30, 2015) (citing *Campbell v. Vaughn*, 209 F.3d 280, 291 (3d Cir. 2000)). Next, the court will consider whether that advice was reasonable under the circumstances of this case under the *Strickland* standard.

At the evidentiary hearing, trial counsel testified that he believed that the victim, *i.e.* the owner of Netrepid, presented as a poor witness to the jury and trial counsel feared that Defendant would come off as equally unsympathetic, if not more so. Trial counsel testified to his reasoning as follows:

> Q. The decision to call [Defendant] as a witness at trial, was there any concern regarding the perception and presenting evidence that [Defendant] was the master of this network?

> A. Yes, there was some concern. There were a number of concerns, and once again, in all candor, [Defendant] is a brilliant young man. However, he does not communicate as well as I would have liked him to, especially when it comes to answering computer related questions. He gets in the weeds, and to a trained litigator that can seem to be deceptive even when it's not, and I was concerned about that.
>
> . . .
>
> So I did send that diagram to him. I sent every diagram that [Defendant] had sent me to Mr. Baker.[5] Mr. Baker and I would discuss them, discuss how we might be able to use them, and if I didn't use it[,] it was probably related to a conversation—I shouldn't say probably. It was related to a conversation with Mr. Baker on strategy versus its effectiveness versus his opinion, and there were many documents that [Defendant] provided that either Mr. Baker said it will not change my opinion or it would confuse my opinion.

(Doc 173-1, pp. 93-4.) Furthermore, as trial counsel noted, if allowed to testify, Defendant would have unequivocally admitted to entering the system and deleting log files, which would have all but assured a conviction:

> Q. Is it fair to say, [Defendant], that if were called to testify at trial by your defense counsel you would have acknowledged that you entered a command or code onto the Netrepid computer system?
>
> A. Yes, I would have.
>
> Q. And you did so without authorization?
>
> A. Correct.
>
> Q. And as a result of putting this command or code onto the computer system you made certain information unavailable?
>
> A. Yes.
>
> Q. And that information that you made unavailable were the logs that you had actually entered the system?
>
> A. That's correct.

[5] "Mr. Baker" was Defendant's expert witness regarding the effects of Defendant's intrusion into the network.

(*Id.* at 229.)

"[W]here counsel's strategic choice rests on several rationale, at least one of which reflects a sound strategic concern, it has been held that even though counsel 'may have been mistaken in part of his legal reasoning[,] [that factor standing alone] does not constitute ineffectiveness where the ultimate strategic choice was reasonable.'" *Campas v. Clark*, No. 17-cv-0682, 2018 WL 4963952, *6 (M.D. Pa. Oct. 15, 2018) (quoting *Druery v. Thaler*, 647 F.3d 535, 540 (5th Cir. 2011)). Trial counsel evaluated not only Defendant's demeanor and his ability to explain the technical distinctions raised by Defendant, but also weighed the relative value of those technical distinctions against the potential for the Government to cross examine Defendant. *See Frederick v. Kyler*, 100 F. App'x 872, 874 (3d Cir. 2004) ("If [defendant's] attorney merely advised him not to testify, that tactical decision certainly would not have fallen below *Strickland*'s standard of objective reasonableness."); *see also United States v. Aldea*, 450 F. App'x 151, 153 (3d Cir. 2011) (finding that counsel's advice not to testify was reasonable where "the risk of exposing [Defendant] to cross-examination" outweighed the potential benefit). Notably, in *Aldea*, the court found it meaningful that the defendant's counsel had performed a thorough cross-examination of the Government's witnesses, as did trial counsel in the present case. (*See e.g.*, TR. at 630-59.) Considering that Defendant would have effectively made a full confession at trial, trial counsel's

advice to Defendant not to testify was reasonable. *United States v. Ruddock*, No. 88-cr-519-23, 1995 WL 717379, *4 (E.D. Pa. Dec. 1, 1995), *aff'd*, 82 F. App'x 752 (3d Cir. 2003) ("[Trial counsel] made a professionally sound decision in advising his client not to testify. Testifying truthfully would have led to a conviction, while [counsel] had an affirmative duty to advise [defendant] not to lie and to withdraw as counsel if he knew that his client would do so.").

The court appreciates the distinction drawn by Defendant between a conviction for a misdemeanor and a felony. Although Defendant would have admitted to a crime, he would not have admitted to causing the full financial loss that would have imposed a felony conviction rather than a misdemeanor conviction. This, however, does not change the court's analysis. Trial counsel's overall strategy was not merely a gamble in which Defendant risked conviction for a felony by trying to escape guilt altogether. Although Defendant would have been able to rebut the allegations that he caused the network failure, trial counsel was concerned with his overall credibility. Essentially, Defendant would have been testifying on his own behalf as an expert witness. As such, the jury would likely have viewed his expert opinion with a "jaundiced eye" in relation to the Government's expert. Simply, trial counsel weighed Defendant's ability to testify to the technical issues now raised in his petition against the harm that would have been caused to his overall case by his admission. It is easy now to question trial

counsel's advice with the benefit of hindsight and a guilty verdict, but absent an express instruction by his client, trial counsel's advice to Defendant not to testify was not unreasonable under the circumstances.

ii. Trial counsel's decision not to present certain evidence

Defendant argues that trial counsel failed to adequately investigate and present as evidence three areas of potentially exculpatory evidence: (1) Defendant's diagram of the Netrepid network configuration; (2) the "Mailbox 100" text message records; and (3) a page from the Billmax manual. As a threshold matter, the court finds that trial counsel adequately investigated the potential impact of each piece of evidence regardless of counsel's decision to actually introduce the evidence at trial. Unlike in several cases cited by Defendant, he does not proffer any evidence that would have been discovered through additional discovery. (*See* Doc 173, p. 26 (citing *United States v. Garvin*, 270 F. App'x 141, 144 (3d Cir. 2008); *United States v. DeCruz*, 2018 WL 585703 (M.D. Pa. Jan. 29, 2018)).) Instead, Defendant argues that the evidence presented to counsel was not fully appreciated by trial counsel or by the defense expert. Counsel presented each piece of evidence to the defense's expert and explained Defendant's position as to their relevancy. *See Snyder v. United States*, No. 07-cr-450, 2013 WL 305604, *4 (M.D. Pa. Jan. 25, 2013) ("[I]n light of Petitioner's own admission of guilt, the Court declines to hold that [petitioner's attorneys] were ineffective for limiting

their investigation to discussions with Petitioner and reviewing evidence presented by the Government."). The defense expert addressed each piece of evidence and determined that they would not impact his opinion.[6] *See Kysor v. Price*, 58 F. App'x 540, 544 (3d Cir. 2002) (finding that trial counsel was not ineffective where counsel declined to pursue insanity defense after presenting evidence to psychiatric expert who advised counsel that pursuing the defense would likely be fruitless); *cf. United States v. Gray*, 878 F.2d 702 (3d Cir.1989) (finding trial counsel ineffective where defendant informed counsel of the identities of two alibi witnesses and counsel did not attempt to subpoena or contact said witnesses). Defendant's argument seems to suggest that trial counsel should have overridden the expert's opinion or fired any expert that disagreed with Defendant's own technical opinion. Trial counsel, as a layperson in the field of computer science, was not unreasonable in relying on his expert's evaluation. As to trial counsel's decision not to introduce the pieces of evidence at trial independent of the expert's testimony, the court will address each argument seriatim.

To rebut the Government's argument that his intrusion into the network caused the overall system crash, Defendant drew a diagram of the network's layout and presented that diagram to trial counsel. Trial counsel presented this drawing to

[6] More specifically, the defense expert testified that a mere diagram was totally insufficient to determine the cause of the network outage. Thus, even had Defendant produced this diagram, his own expert expressly stated that it would not have been sufficient to determine whether Defendant caused the outage. (TR. at 665-66.)

the defense expert but did not introduce the depiction at trial. Defendant argues that the depiction of the Netrepid network presented by the Government gave the jury an inaccurate picture of how the network was set up. Defendant further asserts that this inaccuracy is material to the extent that Defendant's intrusion into the network could have caused the resulting financial loss if the network were configured as depicted by the Government, but not as it actually existed. Even assuming that the diagram was an accurate depiction of the network, trial counsel's decision not to present the diagram was not unreasonable. Trial counsel was aware of the discrepancies and their potential weight at trial. (Doc. 173-1, pp. 72-73.) At the evidentiary hearing, however, trial counsel averred that the drawing was not used expressly because its admission would have required Defendant to testify as to its authenticity, thus subjecting Defendant to the attendant risks of cross examination. As discussed above, the decision not to present Defendant as a witness was a reasonable strategic choice. *See Showers v. Beard*, 635 F.3d 625, 634 (3d Cir. 2011) ("This court agrees that counsel need not, and should not, raise every non-frivolous claim but rather may select among them in order to maximize the likelihood of success on appeal.") (citing *Smith v. Robbins*, 528 U.S. 259, 288, (2000)). Because the introduction of the drawing would have defeated that strategy altogether, trial counsel was not unreasonable in his decision to rely on the defense expert alone.

The court's analysis of the "Mailbox 100" records is nearly identical to its analysis of Defendant's drawing. Defendant averred that, in his role as network administrator, he received text message alerts to his cell phone whenever certain customers reported network connectivity issues or outages. These alerts came through a platform called "Mailbox 100." Defendant stated that he received these alerts not only in the days and weeks following the termination of his employment, but months after. Relevantly, Defendant alleges that he did not begin receiving reports of network outages until 3-4 days after his intrusion into the network. Therefore, he argues, trial counsel should have presented the text message records at trial to show that the outage occurred long after his intrusion. For the same reasons why Defendant could not have been called to the stand to present his network configuration drawing, trial counsel declined to introduce the phone records. Although the parties do not address whether phone records obtained from the cell phone provider could have been authenticated without Defendant's testimony, their import would not have been apparent without Defendant's testimony. Although the introduction of the phone records touches on their probative value as well as counsel's reasonableness, trial counsel held a reasonable belief that the records would have been essentially useless without Defendant's testimony. Although trial counsel could have chosen to present the phone records,

counsel held fast to his strategy not to present Defendant as a witness at trial. *See Clark*, No. 17-cv-0682, 2018 WL 4963952, *6 (citing *Druery*, 647 F.3d at 540).

The final piece of evidence addressed in Defendant's Section 2255 motion gives the court pause compared to the previous two. Unlike the former two proposed exhibits, the Billmax manual would not require Defendant's testimony for authentication. Theoretically, the manual could have otherwise been introduced because it related to a commercial software program that other Netrepid employees and the parties' experts would have been familiar with. Trial counsel's reasoning for not introducing the manual is, however, consistent with his reasoning for declining to introduce the other two pieces of evidence. The defense expert was aware of the manual page, yet did not find it meaningful in creating his expert opinion, and explaining Defendant's alternative theory would have necessitated Defendant's testimony. Although the court does not find trial counsel's decision to be unreasonable, the court will nonetheless address the prejudicial effect of the evidentiary omissions.

iii. Prejudicial effect

Both parties have analogized the instant case to a burglary. The court finds this analogy helpful, but limited. As posited by Defendant, in burglarizing Netrepid's "house," he merely walked up the driveway, opened an unlocked front door and took his own possessions that he had previously left inside. Under the

government's construction, Defendant dug a hole underneath the house's foundation, burrowed through the basement, and left as the house began to crumble and collapse from the foundational instability. It goes without saying that the differences argued by Defendant are no minor distinctions. The issue here, however, is not whether Defendant's assertions, taken as true, could sway the jury. The *Strickland* test asks, in this case, whether the evidence omitted by trial counsel would have been sufficiently persuasive that a reasonable jury would have accepted Defendant's allegations and, thus, rendered a verdict of not guilty. The court finds that the evidence presented by Defendant in his Section 2255 motion fall short of this standard.

As noted in the preceding section, the court did not find counsel's decisions at trial to be unreasonable under the first prong of the *Strickland* test. For completeness, however, the court will address the prejudicial prong of each of Defendant's arguments. The court first examines whether Defendant's proposed testimony would have swayed a reasonable jury. Because the first piece of evidence, Defendant's network diagram, is part and parcel of his own testimony, the court will address those two arguments contemporaneously.

At the evidentiary hearing, Defendant testified as to certain crucial inaccuracies in the network description used by the Government and its experts. In relatively simplistic terms, the network operated by Netrepid was divided into two

parts. There was a public network and a protected network. The former was intended to be publicly accessible to any individuals accessing the internet in order to facilitate web service to Netrepid customers. The latter was intended only to be accessed by Netrepid employees and involved the inner workings of the network. Defendant testified that the networks were protected by firewalls, or programs that acted as gatekeepers, allowing access only to those who were authorized. The firewall protecting the external network allowed presumably only those who were paying Netrepid customers to access the internet. The internal, protected network's firewall was meant to prevent any access to users who did not have proper Netrepid credentials. The Government's depictions of these networks, according to Defendant, were conflated and contradictory. In Defendant's estimation, if the Government's depiction were correct, any internet user would have been able to access the billing and customer information databases operated by Netrepid and, thus, would have access to sensitive customer names, addresses, and credit card information. (Doc. 173-1, pp. 159-61.) Trial counsel testified that he passed the material received from Defendant on to Defendant's expert witness, and discussed it with him, yet the expert did not change his opinion based on this information. (*Id.* at pp. 93-94.)

At trial, the Government's expert directly addressed and refuted the theory now alleged by Defendant, *i.e.* the data deleted by Defendant could not have resulted in the harm caused to the network:

> Q. Let's talk for a moment about some of the derivative effects that these commands might have. You described that there would not only be logs missing as a result of the commands identified in this Government Exhibit 3, but that there would also be files missing?
>
> A. It's—from reading the previous testimony and other documentation related to the case, the commands used, and I don't think you highlighted one of the more interesting commands, the commands used don't differentiate between various types of files. In other words, a removal command, the rm command simply removes a file from the system. It doesn't differentiate between log files, script files, executable files. It doesn't care. It simply deletes a file.
>
> . . .
>
> Q. Is [the rm command] a more—is that different than simply removing of a log?
>
> A. As I've said, the command does not differentiate between log files and other types of files. There's nothing here to indicate that only log files are being deleted, but any file located in that directory.
>
> Q. So any file located in that directory would be gone?
>
> A. That's correct. There was a previous exhibit, I think, introduced yesterday, a demonstrative exhibit that shows a variety of files being stored in that directory. And executing that command would delete all of them.

TR. at 615-16.

Although Defendant analogizes counsel's advice that he not take the stand to a failure to present alibi witnesses at trial,[7] a defendant's testimony that he is

[7] *See, e.g., Moore v. Sec'y Pa. Dep't of Corr.*, 640 F. App'x 159, 163 (3d Cir.), *cert. denied sub nom. Wetzel v. Moore,* 137 S. Ct. 73 (2016) (holding that a failure to call witnesses who would have corroborated defendant's testimony to satisfy the prejudice prong of the *Strickland* test).

innocent of the crimes alleged carries with it an obvious shortcoming compared to a third party witness. It would be a rare defendant that takes his case to trial only to unequivocally admit guilt on the stand. Thus, a jury would view a defendant's protests of innocence as biased and holding relatively little weight. Admittedly, Defendant now appears to exemplify the rare case where a defendant would have admitted, at least in part, to his own guilt. Defendant now avers that he would have effectively confessed to a misdemeanor while acting as his own expert witness in defending against a felony conviction. Nevertheless, a jury would almost undoubtedly view a defendant purporting to be an expert in his own trial with some degree of incredulity.

Any potential prejudice to a defendant must be evaluated in the context of the totality of evidence presented at trial. Here, the Government's case, even limited to the issue of financial loss resulting from the intrusion, was far from weak. *Gregg v. Rockview*, 596 F. App'x 72, 78 (3d Cir. 2015) ("[The *Strickland*] standard is more easily met where the verdict is 'only weakly supported by the record,' as opposed to one with 'overwhelming record support.'") (quoting *Strickland* at 696). The Government's expert was a computer science investigator with the FBI, who taught at the FBI Academy as well as at other academic institutions. The Government expert's position was further supported by testimony from other employees at Netrepid as well as Defendant's former supervisor and the

co-creator of the Netrepid network. Defendant would have been pitting his own expert opinion against the Government's expert, who was unequivocally well-qualified in the field of computer science, as well as other employees who worked directly with the Netrepid network. Defendant's argument relies on the jury making four determinations in his favor: (1) Defendant is a more credible witness than the Government's expert; (2) Defendant is more knowledgeable about the relevant technical issues raised at trail; (3) Defendant was sincere in his testimony that he entered only the commands that he confessed to entering and deleted only the files that the confessed to deleting; and (4) Defendant could not have possibly made an unintentional error, late at night on a Friday evening while dealing with the emotional trauma of having his employment terminated, that would have resulted in additional commands or files being inadvertently deleted. Moreover, Defendant's testimony would have contradicted his own expert's opinion. Thus, Defendant would have been testifying as the sole expert in his defense against the Government's expert or effectively against two experts. Setting aside the strategic implications of such a position, it is unlikely that a reasonable jury would have found Defendant, testifying on his own behalf, and testifying that he was the only person in the world who could know the inner workings of a computer network that he created, as more persuasive than an unbiased expert.

Additionally, it is not entirely clear from Defendant's testimony at the evidentiary hearing what impact the distinctions raised would have. He stated that the network configuration presented at trial was inaccurate, despite testimony that it was a "fair representation of the network," but does not detail how the alleged inaccuracy would have impacted his liability for the financial harm:

> Q. Okay. Would it be possible for a jury to understand what had occurred at Netrepid with a misunderstanding of the configuration or the architecture of the system?
>
> A. No, definitely not.
>
> Q. And why not? Why is that relevant[]?
>
> A. The network looks very what is called flat. There's no layers to it. It's just it's there and there's no indicators of any kind of layers that actually existed in reality versus what's on this piece of paper or that piece of paper

(Doc. 173-1, pp. 167-68.) Stating simply that the jury would not have understood the network functionality without his drawing does little to aid the court in evaluating whether his testimony would have undermined the testimony of other witnesses at trial.[8]

[8]Although not entirely clear, it appears one of the Government's witnesses who worked on the Netrepid network noted that the Government's depiction of the network accounted for the private/public dichotomy now argued by Defendant:

> Q. And Government's Exhibit No. 5. Now is this a network diagram of the various servers that are identified in Government's Exhibit No. 2?
>
> A. Yes.
>
> Q. Now does it divide the various servers identified in Government's Exhibit No. 2 between the public or external servers with the internal servers?

Perhaps the most glaring deficiency with Defendant's proposed testimony, however, is that he likely would have still admitted to a felony under a separate subsection of the CFAA. Under 18 U.S.C. § 1030(c)(4)(A)(VI), a felony conviction can result from "damage affecting 10 or more protected computers during any 1-year period." Defendant testified at the hearing that he entered and deleted log files from ten of the twenty servers. (Doc. 173-1, pp. 217-18.) Assuming Defendant would have testified truthfully at trial, a jury would likely have found Defendant guilty on that alternative ground even if it believed his position as to the liability for the financial harm. In fact, the jury in the present case found specifically that Defendant caused damage to ten or more protected computers, and nothing in Defendant's testimony at the evidentiary hearing would contradict such a finding. (Doc. 95.) [9] Therefore, a finding of causation for the entire financial loss would be relevant only to the amount of restitution owed rather than the felony conviction itself. Accordingly, trial counsel's decision not to have

---

A. Yes.

TR. at 156.

[9]At trial, several witnesses noted that many Netrepid servers were "virtual servers," meaning that they were virtual computers operating on a single physical server "rack." It is unclear how this impacts the ten computer requirement in relation to the definition of a "computer" under the CFAA. Neither party, however, raised this argument at trial or in any subsequent filing, and Defendant's expert agreed that each of the servers accessed by defendant would have been considered separate computers. (TR. at 699.) Moreover, the jury expressly found that ten computers were damaged. (Doc. 95.)

Defendant testify and present his diagram of the network was not prejudicial under the *Strickland* test.

With regard to the Mailbox 100 phone records, the court also finds that trial counsel's decision to omit them from the record was not prejudicial. The theory that rests upon their introduction is not inconsistent with the Government's theory of liability presented at trial. Specifically, the government did not set out to prove that Defendant's intrusion caused immediate irreparable harm to the Netrepid network. Instead, the Government argued that Defendant's intrusion tipped the first "domino" that led to the eventual system crash. The Government's expert opined that Defendant deleted certain files and when individual servers could not locate those files, they experienced errors. Those errors begat other errors which, when compounded, led to the complete network outage experienced by Netrepid. Although the expert did not state how long such a process may have taken, the mere fact that Defendant did not receive notice of the outage until three or four days after his intrusion does not contradict the Government's theory of the case. Moreover, the phone records alone are not a sufficiently reliable indicator of the precise time that the network went down. Defendant testified that only a small subset of users actually availed themselves of the Mailbox 100 system:

> Q. This is a small subset of a small subset out of two thousand.
>
> A. Right. [Internet] residential customers didn't have Mailbox 100 thankfully. Only a subset of business customers had that. And if

> business customers have issues, very likely others were experiencing issues as well, too, different types of customers.
>
> Q. And if business customers were calling in and actually getting somebody on the phone, it wouldn't turn into a voice mail message for you because they're dealing with somebody on the phone.
>
> A. Well, if you're a business customer, you pick up the line, you want to dial the main support number and find out what's going on. If you were not aware that Mailbox 100 existed specifically for you[,] you wouldn't be calling it.

(Doc 173-1, p. 241.) Thus, it is entirely possible that residential customers experienced more immediate outages that were reported via other means. It may also have simply been the case that the business customers were not at work over the weekend to experience and report the outages. Defendant's intrusion took place on a Friday night and many businesses do not operate on Saturdays and Sundays. It is true that Defendant has asserted theoretical arguments that may have supported his case if introduced at trial; however, these evidentiary elements are insufficient to meet the second prong of the *Strickland* test.

Finally, as acknowledged above, the third piece of evidence referred to by Defendant in his Section 2255 motion, the BillMax manual page, could have been introduced without requiring Defendant to take the stand. Similar to his arguments relating to his own testimony and his network diagram, Defendant argues that the information contained in this manual would have shown that the data he deleted could not have possibly led to the network crash. Defendant's own expert witness reviewed the manual and did not concur with Defendant's assessment. Aside from

that expert's opinion, the Government's expert again appears to have addressed this argument at trial and refuted it.

> Q. With the command or commands that you just previously described, if those command or commands were placed on any particular server, what would the impact be if that server had scripts such as this?
>
> A. Let's see. This script appears to be trying to restart the Billmax server at some point here, a portion of the script that, I guess, deals with the Billmax system. I'm not sure what the impact would be on this particular script. It's related to the MySQL service here. My understanding is the Billmax system relies on the MySQL database system.
>
> Q. You said it's your understanding that the Billmax's service relied upon the MySQL?
>
> A. MySQL database system, particularly the service.
>
> Q. Let's talk about the MySQL database. Can you explain for the jury your understanding of the MySQL database and its relationship with a RADIUS server and Billmax?
>
> A. I did some investigation into the Billmax system. I've looked into various issues with the MySQL server. Reviewing open source documentation on the Billmax system, it can and does rely on the RADIUS server operation. It can use the RADIUS server in a way to log when a user attempts to authenticate with the system therefore informing the Billmax system when a user attached himself or herself to the environment for authentication, and therefore the Billmax system then billed them on an hourly basis or whatever noting how long they were on the system. The RADIUS server provides that connection for the user. The RADIUS server uses a MySQL database to authenticate users and then can create a log that the Billmax system then would use to note when that user connected to the environment.
>
> Q. Can you describe for the jury what would be the effect if a Cron job were placed on the MySQL database causing logs or files or file directories to be erased from the MySQL database?
>
> A. If that particular Cron job was placed on the server that controlled the authentication using MySQL, it would delete the MySQL logs.

> An open source investigation that I conducted would indicate that that service could be detrimentally affected. That deleting the log file could shut down the MySQL service and keep it from running.
>
> Q. So by having the logs, log files removed from the MySQL database, could have the effect of shutting down the MySQL database from functioning?
>
> [A]: Yes, sir.

TR. 617-19. In contrast, when questioned regarding the BillMax manual at the Section 2255 hearing, Defendant explained:

> A. Yes. Dr. Ates testified that he had read and got familiar with the BillMax documentation and proceeded to testify saying that log file deletion of files located within slash bar slash logs would have damaged BillMax, rendered it inoperable.
>
> Q. And where on this document, is it the second page?
>
> A. In this document it says the output of log files for BillMax, this is a BillMax manual.
>
> Q. Okay.
>
> A. It says the log files are stored in slash USR slash local slash BillMax slash logs specifically.
>
> Q. Okay. So what is this saying where are those logs stored?
>
> A. It's saying log files related to BillMax are stored in a completely different location.
>
> Q. Than?
>
> A. Than from where I deleted the log files I deleted.
>
> Q. Okay.
>
> A. And it [sic] had Dr. Ates actually read the manual he would have also on Chapter 2 seen that BillMax's files are stored in a few locations, none of which are in slash var slash logs. Specifically on the BillMax server they're in OPT BillMax, or as I just said previously in the previous statement their files are stored in slash USR, which U-S-R, slash local slash BillMax, as well as the BillMax database, which is again everything that's in a completely different directory than what system logs are stored in.

> Q. Okay so there is, does the BillMax manual support your testimony that the log files you removed in Homer slash BillMax could not have harmed BillMax?
>
> A. Correct.

(Doc. 173-1, pp. 182-84).

At most, this testimony would result in a "battle of the experts," as the Government's expert testified that he reviewed the relevant Billmax documentation and found that the files deleted by Defendant could have affected the Billmax system. Although the evidence now raised by Defendant, taken together with his testimony, would have lent some support to his arguments at trial, they fall short of demonstrating "a reasonable probability that but for the error, the jury would have acquitted him." *Kysor v. Price*, 58 F. App'x at 545. Accordingly, the court finds that Defendant also fails to satisfy the prejudice prong of the *Strickland* test.

IV. Conclusion

For the reasons set forth above, the court finds that the Government was required to demonstrate actual financial loss rather than simply damage in the form of the deletion of computer files. The court further finds that Defendant's trial counsel was not ineffective because Defendant did not demonstrate that counsel acted unreasonably in investigating and presented evidence at trial or advising Defendant not to testify. Additionally, the court finds that, even if trial counsel had acted unreasonably, the alleged errors did not prejudice Defendant at trial under the *Strickland* test. Accordingly, the court will deny Defendants Section 2255 motion.

An appropriate order follows.

s/Sylvia H. Rambo
SYLVIA H. RAMBO
United States District Judge

Dated: December 12, 2018